(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/23831 A1

(51) International Patent Classification[7]: H04L 12/56, 12/14, H04Q 7/22, G06F 17/60

(21) International Application Number: PCT/SE01/01924

(22) International Filing Date:
10 September 2001 (10.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0003275-5 15 September 2000 (15.09.2000) SE

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET L M ERICSSON (publ)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KANNAS, Chris** [AU/SE]; PL 3245, Ornunga, S-447 93 Vårgårda (SE). **SUNDELL, Hans-Olof** [SE/SE]; P.O. Box 17, Kalvsund, S-430 90 Öckerö (SE). **CARLSSON, Niclas** [SE/SE]; Plåtslagaregatan 6A, S-417 57 Göteborg (SE). **MÅRDBERG, Elisabet** [SE/SE]; Sanatoriegatan 31A, S-416 53 Göteborg (SE). **WILLIAMS, Brian** [AU/AU]; 11 St. Georges Court, Greensborough, Melbourne, 3088 (AU).

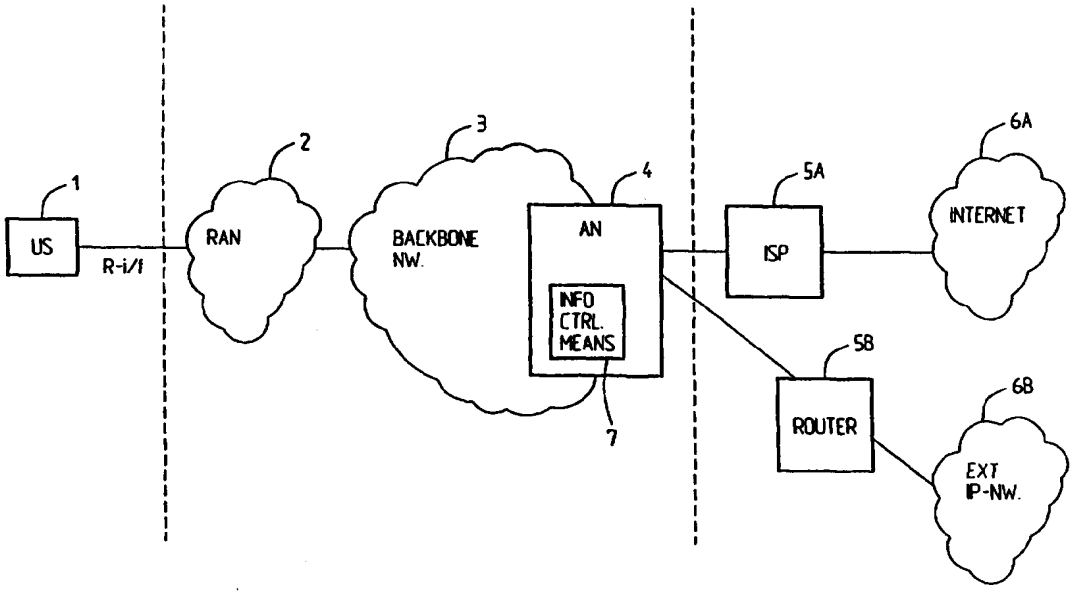
(74) Agents: **BERGENTALL, Annika** et al.; Cegumark AB, P.O. Box 53047, S-400 14 Göteborg (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF,

[Continued on next page]

(54) Title: ARRANGEMENT AND METHOD FOR FILTERING DATA COMMUNICATION



(57) Abstract: The present invention relates to an arrangement and to a method in a communication system supporting communication of packet data with a number of end user stations (1), a backbone network (3), a number of access means (4) for providing access between end user stations (1) and external packet data networks (6A, 6B). Information control means (7) are provided. Said information control means (7) are end user controlled such that an end user (1) selectively can control the reception of data packets from the external packet data network(s) (6A, 6B).

WO 02/23831 A1

CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Title:

ARRANGEMENT AND METHOD FOR FILTERING DATA COMMUNICATION

FIELD OF THE INVENTION

The present invention relates to controlling the transfer of data packets between external packet data networks and end users of a communication system supporting communication of packet data. Particularly it relates to an arrangement in a (mobile) communication system supporting communication of packet data with a number of end user stations, a backbone network and a number of end user access means for providing access between end user stations and external packet data networks, which comprises information control means.

The invention particularly also relates to a method of controlling the communication of data between a number of external IP networks and an end user station in a communication system comprising a backbone network supporting communication of packet data.

STATE OF THE ART

The usage of Internet services is growing rapidly and the number of end users attached to the Internet is also growing very rapidly. This makes it possible to distribute for example information and advertisements to a large number of end users in a very simple manner. However, the situation may occur that the distributed information or the advertisement etc. is not wanted by the end user. An end user actually runs the risk of being flooded by unwanted information. In addition to being extremely annoying for the end user, the end user may be charged for the

time the end user or the mobile host is connected to for example an ISP (Internet Service Provider), and, even worse, is charged based on the amount of data the mobile host or the end user receives from the external data network. The end user may also be charged for the amount of data that is transmitted to the external network. However, the end user has means to control the transmission of data but he has, today, absolutely no control as far as the reception of data is concerned. The consequence thereof will be that the user of the mobile host or the mobile station does not have any control of the costs, which is a serious problem. When a mobile end user station or a mobile host is connected by radio, over an air interface, to for example a backbone network, or generally within the wireless community of data communication, the bandwidth for transferring data to and from a mobile host is limited due to the air interface.

Thus, the problems relating to charging are considerable. Moreover, a user of a mobile host may be swamped by unwanted data, such as for example unwanted push advertisements which clearly also is not desirable. Furthermore, the transmission of data that actually is not wanted by a user, indeed is a waste of network resources.

These problems also exist in the fixed data communication community, but, in this environment, charging is generally not based on volume. However, it may well be volume based in the future and therefore also for a fixed data communication community similar problems may arise also as far as charging is concerned.

The only means available today to somehow control the distribution of packets to an end user, is provided by, in the case of Internet, the Internet Service Provider (ISP) which is the end user access point to the Internet or any other external network wherein some packet filtering technology may be implemented. This means however that firewalls may be configured for the whole network which is very inflexible. It would also be possible, if a particular end user does not want to receive some particular information, that an operator manually stops the traffic from a given origin or similar. This however presupposes that an end user actively informs the operator through a complaint or similar. Generally, any control procedures handled by the operator, are implemented for a whole network. Such solutions are not satisfactory since they are not simple and they involve high costs per se. Consequently, with today known control means, an increasing number of end users will still receive, and pay for, unwanted information, advertisements etc. Another serious problem is when someone abuses the system and maliciously sends (large amounts of) information to one or more end users resulting in the end user actually having to pay for the malicious action, and the end user might not even be able to receive the information he actually wants to receive.

SUMMARY OF THE INVENTION

What is needed is therefore an arrangement through which the control of distribution of information, advertisements etc. to an end user can be improved or rather provided for. An arrangement allowing a flexible control of the distribution of information to end users is also needed. Generally an arrangement is needed through which it is prevented that an end user or a mobile host has to pay for unwanted information or for the time he/it is connected due to transfer of unwanted

information. Moreover an arrangement is needed through which the network resources are not unnecessarily used for transfer of unwanted information and through which network resources thus can be saved. An arrangement is also needed through which can be prevented that a mobile host, or a fixed host, be swamped by unwanted data such as for example unwanted push advertisement or similar. An arrangement is also needed through which abuse can be prevented, or at least that the consequences for an end user due to malicious actions can be reduced. A method of controlling the transfer of data is also needed through which one or more of the above mentioned objects are fulfilled.

Therefore the present invention provides an arrangement in a communication system, particularly a mobile communication system, which supports communication of packet data, and which comprises a number of end user stations, a backbone network, a number of end user access means (points) or access nodes for providing access between end user stations and external packet data, e.g. IP networks or X.25 networks. Information control means are provided which are end user controlled such that an end user selectively can control the reception of data packets from the external packet data network(s) over the access node. The end user stations are particularly connected to the backbone network over a radio interface. The end user stations may be mobile as well as fixed. The invention actually also covers the case when they are not connected by radio to the backbone network but where similar problems still may be present, e.g. for any of the reasons discussed above, such as volume based charging. The external packet data network may be the Internet but it may also be other external IP networks such as corporate LANs (Local Area Network) or X.25 networks etc.

The information control means particularly comprises an optional, end user remotely defined or set up filter. In a most advantageous implementation the filter is provided in the access means, also called an access point or an access node, to an external packet data, e.g. IP network. By provided it is here particularly understood that it is defined, or set up, and activated in the access means.

For external packet data network, e.g. IP network, access, the access means are connected to a router, which, for Internet access, may be an ISP (Internet Service Provider). For other packet data networks it may be other routing means; the external network may also be a PLMN (Public Land Mobile Network) or any other network routed through for example an ISP.

Particularly the filter is defined by the end user, and to obtain the desired filtering functionality, a number of filtering function attributes are used to define the customized filter. For activating/defining (setting up) such a customized filter, a message signal is provided from the end user station by the end user wanting to implement a filtering functionality. The message signal is sent from the end user station (mobile host) to the access means or the access node.

According to one embodiment a specific or a new message is created for defining and/or activating the filter. In another embodiment, according to a generally even more advantageous implementation, an already existing message signal is used for setting up the desired filter functionality. It may for example relate to a standardized message that is used (also) for a new purpose and which is provided with information about the filter

requirements, i.e. the filtering function attributes which most advantageously are defined or given by the end user, such that a particular end user can create a filter according to his specific needs substantially at any time. The end user can also remove (shut off) the filter, change the filter requirements etc. using existing messaging provided with supplemental information or through the creation of entirely new signals or messages.

This provides the user with an efficient and flexible means to set up a filter if he for example detects that someone maliciously transfers a lot of information to him or if large amounts of more or less uninteresting information is sent to him or whatever the reason may be for not wanting to receive some particular information (or all information except some particular information).

The filtering functionality may be positive or negative, i.e. defining either wanted information or unwanted information. If it is based on which of information an end user actually does want to receive, the filter may be set up according to the principles of merely allowing some specific information whereas filtering out all other information.

The filtering functionality can be defined in many different manners. The filtering function attributes may be of many different kinds and herein merely some examples on attributes will be given. They may for example relate to one or more of source IP address, IP subnet, source port in IP header, source type of protocol in IP header, originating router, ISP or any other router, FTP files etc. This means for example that an end user can select to filter out all information with a given

source IP address, but it is also possible to filter out information from an entire subnet etc.

Generally the definition/activation of a filtering functionality, i.e. setting up of a filter, presupposes a successful connection or attachment by an end user station to the backbone network. This is so because only then the end user address will be known such that packets received in the access means having a destination address corresponding to the address of the end user having defined or set up a filter, are exposed to the filter. This means that the filter is implemented on all packets addressed to the concerned end user station (received over the concerned access node).

In a particular implementation the network comprises a GPRS or a UMTS/GPRS system. The access means may comprise a GGSN (Gateway GPRS Support Node). In that case the existing messaging relating to activation and set up of a secondary PDP context request/response are with advantage used for the setup of a filter in GGSN. Such messages are then provided with information relating to the filter attributes, a service class with the context of discarding unwanted data packets not meeting the filter requirements given by the filter parameters. However, it is of course also possible to create new messages for the filtering functionality setup. Of course the concept may also be implemented on other systems supporting communication of packet data such as for example PPDC, CDPD etc.

In one particular implementation the access means comprises or are associated with a more or less conventional firewall and the filter is then set up, defined and activated, in the firewall.

The invention also discloses a method of controlling the communication of data between a number of external IP networks and an end user station in a communication system comprising a backbone network and supporting communication of packet data. The method includes the steps of; controlling the reception of data in the end user station through: providing information from the end user station to external packet data network access means containing requirements relating to wanted/unwanted data information; defining and activating control means in the access means (or access node) such that only wanted data information is forwarded to the end user. The control means particularly comprises a filter. The method advantageously further includes the steps of; creating a new message for providing the information for defining/activating the control means from the end user station to the access point. In an alternative implementation the method includes the steps of; using existing signalling/messaging from the end user station to the access means for providing the information for defining/activating the control means.

In a particular implementation the backbone network is (UMTS) GPRS and the method includes the steps of; using the messaging relating to requesting and activating a secondary PDP context to setup information control means comprising a customized filter in an access point comprising a GGSN. Particularly the method also includes the step of applying the filter on all data packets received in the access means having the address of the end user having activated/defined the filter as destination address and discarding unwanted data packets or only allowing wanted data packets to pass through the filter.

It is an advantage of the invention that through the information control means the end user actually gets control over what he wants to receive and what he does not want to receive since they are actually remotely controlled and manipulated by the end user himself. This makes it both more flexible, cheaper and quicker to install than it would be through any kind of operator controlled filter means. It is also an advantage that, in one embodiment, existing messaging can be used. Then it is very easy to implement the functionality, without awaiting any amendments to standards etc. which is important since the problems for end users relating to reception of unwanted data, particularly as far as charging is concerned presumably will be even more serious in the future. It is also an advantage that not only an end user can introduce a filtering function, he can also remove a filtering function, modify the filtering function etc.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will in the following be further described in a non-limiting way and with reference to the accompanying drawings in which:

Fig. 1 very schematically illustrates a wireless data communication system wherein information control means are provided in access means towards external IP networks,

Fig. 2 very schematically illustrates a UMTS/GPRS system to which the inventive concept can be implemented as above,

Fig. 3 in a simplified way indicates messaging between a user station and an access point for remote setup of a filter,

Fig. 4 illustrates the PDP Context Activation Procedure for GSM,

Fig. 5 is a figure similar to Fig. 4 but for UMTS,

Fig. 6 illustrates the Secondary PDP Context Activation Procedure for GSM,

Fig. 7 is a figure similar to Fig. 6 but for UMTS,

Fig. 8 illustrates one embodiment of the invention as implemented on UMTS/GPRS and using existing messaging and,

Fig. 9 is a flow diagram describing the embodiment of Fig. 8.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 very schematically illustrates a communication system supporting wireless communication of data. A wireless host, here called User Station US 1 is via a radio interface connected to a radio network RAN 2 which communicates with the backbone network 3. The backbone network 3 comprises a number of access points or Access Nodes AN 4 which here generally are denoted access means, of which only one is illustrated in the figure, for the provision of access between User Stations US 1 and external packet data networks 6. The Access Node AN 4 communicates with a router 5B and an ISP 5A for routing traffic to/from external IP

networks 6A,6B. An example on an external IP network is the Internet 6A; it may also be a corporate LAN etc or an X.25 network. For Internet, the routing means 5A comprises an ISP (Internet Service Provider). Generally the user station 1 needs to perform signalling to for example a base station (not shown) in the fixed part (BSS) of the backbone network 3 to get access to said backbone network 3. When access has been provided, according to the present invention, the user station 1 may send a message, a new message or an already defined message with supplementary information, to the Access Node AN 4 to set up a filter (information control means 7) in, or in means associated with, said access node. Information relating to the filtering requirements are included in or added to the message or sent in a subsequent message; the invention is not limited to any particular way of doing this, the important thing being that the user station 1, i.e. the end user, is able to initiate the setup of a filter so as to enable the user to determine what information he wants to receive or what information he does not want to receive without interference or assistance by any operator or without requiring that the operator handles the filtering procedure.

Fig. 2 is a figure similar to that of Fig. 1 but relating to a particular embodiment in which the backbone network is the GPRS/UMTS as standardized for example in 3G TS 23.060, v3.4.0 (2000-07) Technical Specification 3GPP™ and TS 24008 v3.4.1 (2000-07), 3GPP.

In Fig. 2 a user station 11 is shown which comprises a computer connected to a mobile station MS which in turn is connected to the backbone network 31, here comprising UMTS/GPRS, over a radio interface connected to a radio network RAN 21 which in turn

communicates with a SGSN 29 (Serving GPRS Support Node), c.f. e.g. TS 04.64 v5.1.0 (1997-12) which describes the MS-SGSN and GPRS. SGSN 29 is over the backbone network 31 connected to a GGSN 41 (constituting the access node) which is a gateway GPRS support node. The GGSN 41 is connected to a router 51, for routing to an external IP network 61, e.g. Internet. If the external network 61 is the Internet, the router 51 may be an ISP as discussed above. To the external network 61 a number of hosts or servers 62A, 62B are connected, only two of which are shown for reasons of simplicity and which IP network users may access.

US 11 has to signal to a base station (not shown) in the backbone network 31 in the fixed network part of the system. In GPRS and UMTS systems this is performed by the user station US 11 executing an attach procedure to get access to the GPRS/UMTS network, followed by the PDP context procedure to get access to an external network via an ISP or more generally via a router. The attach and PDP context procedures are described in the above mentioned references and will also be more thoroughly explained below.

The inventive concept is applicable to any systems supporting communication of packet data and in which end users may face the problem(s) initially referred to.

In Fig. 3 is shown in a very simplified manner how messages are sent to provide for end user controlled filter setup. It is here supposed that access or connection already has been provided between the user station and the backbone network before a filter can be set up, although this is not the case if the user station is a fixed station. It is hence supposed that a Set User Station (US) filter request is sent from the User Station (US)

to the access point or access node AN. In an advantageous embodiment the request contains a list of parameters defining the filter requirements, i.e. which packets should be allowed and which should not be allowed respectively for further forwarding from the external network towards the end user having set up the filter. Thus, the end user of a user station can inform the access means to set up a customized user profile. The access node then uses the information from the user station to set up the user packet filtering function in the Access Node AN accordingly. When the filtering functionality has been set up in the access node, a set US filter response is returned from the Access Node AN to the User Station US. When the filter has been setup, the end user can control which data that is to be received from one or more external networks and thereby obtain control of received, and, if applicable, charged data and information, which is extremely advantageous.

Optionally a security function may be included which, after a filter request has been received in the access node, is performed through signalling between user station and access node in any appropriate or known manner. If the user station passes the optional security function, the access node proceeds to setting up the user customized packet filtering function.

After the filter function has been set up, i.e. defined and activated, in the Access Node AN, the data traffic from the external network, which matches the attributes of the filtering function, will be discarded in the access node. The end user may of course use a number of different attributes to set up the user profile in the access node. Below some examples are given: source IP address or subnet in the IP header; source port number in the IP header; source type of protocol in the IP header, from

which router, or particularly ISP, the IP packet is received etc. It is also possible to, for example, filter out FTP (File Transfer Protocol) packets. The filtering functionality may be implemented in different access nodes providing access to one or more external IP networks.

Below, and with reference to Figs. 4-8, particular embodiments relating to GPRS/UTMS will be more thoroughly discussed in which already existing messages are used for the provision of a user defined and activated filter. As referred to above, however, it is also possible to create new messages specifically for the intended purpose.

According to the invention, it is possible to implement the invention to the 3GPP 23.060 standard with a minimum impact. The messages "activate secondary PDP context request/response" can be used to set up a "no service traffic class" and a "waste basket context". The message request will then particularly contain a new QoS (Quality of Service) value identifying such a "no service" request. Furthermore the message preferably contains a TFT (Traffic Flow Template) specifying the user defined filter attributes which can be said to act as a firewall stopping packets according to requirements but letting others pass.

Quality of Service (QoS) comprises a quality of service information element specifying the QoS parameters for a PDP context (PDP is a Packet Data Protocol such as for example IP). Quality of Service is further described in 3G TS 24.08. v3.4.1 (2000-07) by 3GPP which herewith is incorporated herein by reference. In the above mentioned 3G TS 23.060 v3.4.0 (2000-07) by 3GPP, and which also is incorporated herein by reference, PDP

context activation, modification, deactivation and preservation functions are described in section 9.2 of chapter 9, Packet routing and transfer functionality.

For example does a GPRS subscription contain the subscription of one or more PDP addresses. Each PDP address is described by one or more PDP contexts in the MS, the SGSN and the GGSN. Each PDP context may be associated with a TFT and at most one PDP context associated with the same PDP address may exist at any time with no TFT assigned to it. The reason for having several PDP contexts per PDP address is to get different QoS:s, one for each such PDP context. A PDP context is established with a particular QoS. TFT differentiates the traffic so that each packet gets the appropriate QoS. Every PDP context exists independently in one of two PDP states. The PDP state indicates whether data transfer is enabled for that PDP address and TFT or not. In case all PDP contexts associated with the same PDP address are deactivated, data transfer for that PDP address is disabled.

In an inactive state, the data service for a certain PDP address of this subscriber is not activated. Then no data can be transferred relating to that PDP address. An MS may initiate the movement from an inactive to an active state by initiating a PDP Context Activation procedure. In the active state, the PDP context for the PDP address in use is activated in MS, SGSN and GGSN.

A GPRS- attached MS can initiate activation, modification and deactivation functions at any time for a PDP context in the MS, the SGSN and the GGSN. Upon reception of an Activate PDP Context Request message or an Activate Secondary PDP Context Request message, the SGSN initiates procedures to set up PDP contexts.

The messaging briefly referred to above can be used to implement the inventive concept in that when the backbone network, i.e. here GPRS/UMTS, receives and activates a Secondary PDP Context Request, it will, according to the invention, recognize the new "no service" traffic class and then pass the request on to the GGSN via the Create or Activate PDP Context Request without setting up any bearer resources, such as for example GTP tunnels and radio bearer. The GGSN then creates a "waste basket context", i.e. a context according to which packets not to be forwarded to the end user having defined and set up a filter, be discarded. Filter attributes coupled to the waste basket context are stored in GGSN. Any downlink user packets matching the defined filter attributes will then be directed to the waste basket context and discarded by the GGSN node.

For the activation procedures referred to above reference is again made to 3G TS 23.060 and in Fig. 4 the PDP context activation procedure for GSM is described. First the MS, corresponding to the User Station US, sends an Activate PDP Context Request (1_G) to the SGSN. The MS shall use the PDP Address to indicate whether it requires the use of a static PDP Address or whether it requires the use of a dynamic PDP Address. The MS may use the access point name to select reference point to a certain external network and/or to select a service. Access point name is a logical name referring to the external packet data network and/or to a service that the subscriber wishes to connect to. QoS Requested is a parameter included in the request and it indicates the desired QoS profile. PDP Configuration Options may be used to request optional PDP parameters from the GGSN. PDP configuration options is sent transparently through the SGSN. (1_G of Fig. 4).

In GSM security functions may be executed, (2_G). This, however, is not necessary for the functioning of the present invention. It should be noted that some of the messages which are not substantially relevant for, or affected by, the implementation of the inventive concept, are not illustrated in the Figures.

SGSN validates the Activate PDP Context Request using PDP type (optional), PDP address (optional), and Access Point Name (optional) provided by the MS and the PDP context subscription records. The validation criteria, the APN selection criteria and the mapping from APN to GGSN is described further in the above mentioned technical specification. The SGSN sends a Create PDP Context Request (PDP type, PDP address, Access Point Name, QoS negotiated etc.) message to the affected GGSN. Access Point Name shall be the APN Network Identifier of the APN selected. PDP address shall be empty if a dynamic address is requested. The GGSN may use Access Point Name to find an external network and optionally to activate a service for this APN. GGSN creates a new entry in its PDP context table and generates a charging ID. The new entry allows a GGSN to route PDP PDUs between the SGSN and the external PDP network and to start charging. The GGSN then returns a create PDP context response message, (3_{G2}), including among others PDP address, PDP Configuration options, QoS negotiated etc. to the SGSN. The Create PDP Context messages are sent over the backbone network. Thus, according to the present invention these messages can be used and modified as referred to above, to contain a value for QoS identifying a new "no service" request and a TFT specifying filter attributes as defined by the end user.

According to GSM, BSS (Base Station Subsystem) packet flow context procedures may be executed; this is however not of importance for the present invention.

The create PDP Context Request and Response messages (3_{G1}), (3_{G2}) are sent between SGSN and GGSN, and GGSN and SGSN respectively. Finally, (4_G), the SGSN inserts NSAPI (Network layer Service Access Point Identifier) together with the GGSN address in its PDP context. If the MS has requested a dynamic address, the PDP address received from the GGSN is inserted in the PDP context. The SGSN selects radio priority and the packet flow ID based on QoS negotiated and returns an activate PDP Context Accept message (4_G) to the MS.

The SGSN is able to route the PDP PDUs between the GGSN and MS and starts charging. According to the present invention, having introduced a filtering functionality into GGSN for downlink communication, packets matching the user defined filter attributes will be directed to the "waste basket" context and discarded by the GGSN node as discussed above.

In Fig. 5 the PDP Context Activation procedure for UMTS is described. The message (1_U), i.e. the Activate Context Request is just like for GSM, sent from MS to SGSN wherein SGSN in this case is an SGSN-U, i.e. an SGSN supporting UMTS. In other aspects it is similar to (1_G) for GSM. In UMTS, Radio Access Bearer setup is performed by the RAB assignment procedure as described in 3G TS 23.060 as referred to above. This is however not of importance for the present invention, like any security options (not shown). Also the create PDP Context Request and Create PDP Context Response messages (3_{U1}), (3_{U2}) are similar to

the messages (3_{G1}), (3_{G2}) described with reference to GSM above as is the Activate PDP Context Accept Message (4_U).

The Secondary PDP Context Activation procedure may be used to activate a PDP context while reusing the PDP address and other PDP context information from an already active PDP context, but with a different QoS profile. The Secondary PDP Context Activation procedure for GSM is described in Fig. 6 whereas the procedure for UMTS is described in Fig. 7. Thus, with reference to Figs. 6 and 7 the Secondary PDP Context Activation procedures as standardized are described whereas in Fig. 8 an inventive implementation is described according to which the secondary PDP Context Activation procedure is used to set up a filter in GGSN.

According to Figs. 6 and 7, the procedures for APN selection and PDP address negotiation are not executed. Each PDP context sharing the same PDP address and IPN shall be identified by a unique TI and a unique NSAPI. The Secondary PDP Context Activation procedure may be executed without providing a Traffic Flow Template (TFT) to the newly activated PDP context if all other active PDP contexts for this PDP address and APN already have an associated TFT, otherwise a TFT shall be provided. The TFT contains attributes that specify an IP header filter that is used to direct data packets received from the interconnected external packet data network to the newly activated PDP context.

The Secondary PDP Context Activation procedure can only be initiated after a PDP context is already activated with the same PDP address and APN.

Fig. 6 illustrates the Secondary PDP Context Activation procedure for GSM. First the MS sends an Activate Secondary PDP

Context Request message to the SGSN including information related to linked TI, NSAPI, TI, QoS Requested, TFT, wherein linked TI indicates the TI value assigned to any one of the already activated PDP contexts for the concerned PDP address and APN. QoS Requested indicates the desired QoS profile. TFT is sent transparently through SGSN to GGSN enabling packet classification for downlink data transfer. TI and NSAPI contain values not used by any other activated PDP context ($1'_G$).

Security functions ($2'_G$) are optional in GSM but since it is irrelevant if such are implemented or not for carrying out the inventive concept, they are not further discussed herein. Then SGSN validates the Activate Secondary PDP Context Request using the TI indicated by linked TI. The same GGSN address is used by the SGSN as for the already activated PDP context or contexts for that TI and PDP address. SGSN and GGSN may restrict and negotiate the requested QoS as in the PDP context activation procedure. The SGSN sends a Create PDP Context Request (QoS negotiated, TEID, NSAPI, primary NSAPI, TFT) message ($3'_{G1}$) to the concerned GGSN. Primary NSAPI indicates the NSAPI value assigned to any one of the already activated PDP contexts for the PDP address and APN. TFT is included only if received in the Activate Secondary PDP Context Request message. GGSN uses the same external network as used by the already activated PDP context(s) for the concerned PDP address, generates a new entry in its PDP context table, and stores the TFT. The new entry allows the GGSN to route PDP PDUs via different GTP tunnels between the SGSN and the external PDP network. The GGSN returns a Create PDP Context Response message to the SGSN ($3'_{G2}$). Further procedures may be executed which however are not relevant for implementing the present invention.

Finally the SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated and returns an Activate Secondary PDP Context Accept message ($4'_G$) to the MS.

Fig. 7 is a Figure similar that Fig. 6 with the difference that in UMTS, Radio Access Bearer is performed through the RAB Assignment procedure ($2'_U$). The messaging ($1'_G, 3'_{G1}, 3'_{G2}, 4'_G$) of Fig. 6 corresponds to the messaging ($1'_U, 3'_{U1}, 3'_{U2}, 4'_U$) for UMTS.

In Fig. 8 the use of the Secondary PDP Context Activation procedure messaging to implement the inventive concept will be described. The Mobile Station MS, corresponding to the User Station US, sends an Activate Secondary PDP Context Request to SGSN combining parameters QoS = O, TFT = filter, and contains filter attributes, 10. SGSN sends a PDP Context Request (QoS = no service, TFT = filter, all attributes) 20_1, to GGSN. No bearer resources are setup or requested. In GGSN a waste basket context is setup. The GGSN sends a PDP context response 20_2 to SGSN which sends a activate Secondary PDP Context Accept 30 to the user station US. The filtering function is then implemented on all downlink user packets such that if the packet characteristics match with TFT filter attribute criteria, the packet is directed to waste basket context for discarding by the GGSN.

Thus, according to the invention an end user of a mobile host is provided with means to control the reception of (un)wanted data and an end user can set up a desired filter profile remotely. The user profile contains the filtering function attributes. The filter can be reset or modified whenever the end user so wants.

Fig. 9 is a flow diagram illustrating the procedure for a user controlled, remote setting up of a personal filtering profile.

In the flow diagram of Fig. 9 it is first supposed that end user A wants to obtain control over the reception of data from external IP networks. The reason therefore may be that it is detected that packet are sent maliciously, that end user A simply receives too many packets which end user A is not interested in, that A simply wants to limit the reception of data or that A wants to receive data for example only from a particular source or for any other reason. End user A performs an attach procedure for attachment to the backbone network, 101, if this was not already done before. Subsequently end user A initiates a PDP Context Activation procedure, 102, as further discussed above with reference to for example Fig. 4 or Fig. 5.

Then end user A sends an Activate Secondary PDP Context Request to SGSN with a new QoS value relating to "no service" and TFT specifying filter attributes such as for example source IP address or one or more of the other filter attributes referred earlier in the application or any other appropriate attribute or attributes, 103. This request is received in SGSN; SGSN sends a Create Secondary PDP Context Request with the above mentioned QoS and TFT to GGSN, 104, as also discussed earlier. Subsequently the filtering functionality according to the user defined requirements is setup in GGSN, with a context relating to disposal of packets with specified attributes, 105. A response message relating to the creation of a PDP Context is then provided from GGSN to SGSN, 106. From SGSN a confirmation message relating to acceptance of the activation of a Secondary PDP Context is sent to the user station of end user A, 107. Then the filter is applied on all data packets from the external network(s) containing the destination address of end user A, 108. Unwanted packets are then discarded in GGSN, 109.

It should be clear that the invention is not limited to the particularly described embodiments but that it is applicable to all communication systems supporting communication of packet data from external networks to an end user, particularly relating to wireless user stations but also to fixed stations if similar problems are present, for example as far as charging is concerned but also more generally if an end user wants to obtain control over the reception of wanted and unwanted information.

CLAIMS

1. An arrangement in a communication system supporting communication of packet data with a number of end user stations (1;11), a backbone network (3;31), a number of access means (4;41) for providing access between end user stations (1;11) and external packet data networks (6A,6B;61),
c h a r a c t e r i z e d i n
that information control means (7;71) are provided, that said information control means (7;71) are end user controlled and comprises an optional end user defined and end user activated filter, such that an end user (1;11) selectively can control the reception of data packets from the external packet data network(s) (6A,6B;61).

2. An arrangement according to claim 1,
c h a r a c t e r i z e d i n
that the end user station(s) (1;11) is/are connected to the backbone network (3;31) over a radio interface.

3. An arrangement according to claim 1 or 2,
c h a r a c t e r i z e d i n
that the end user station(s) is/are mobile.

4. An arrangement according to claim 1 or 2,
c h a r a c t e r i z e d i n
that the end user station(s) is/are fixed.

5. An arrangement according to any one of claims 1-4,
c h a r a c t e r i z e d i n

that the/an external packet data network is an IP-network (6A) e.g. the Internet.

6. An arrangement according to any one of the preceding claims, c h a r a c t e r i z e d i n that the external packet data network(s) comprises (a) corporate LAN(s).

7. An arrangement according to any one of the preceding claims, c h a r a c t e r i z e d i n that the end user setup filter is provided in an access means (4;41), i.e. an access point, to an external packet data network, e.g. an IP-network.

8. An arrangement according to claim 7, c h a r a c t e r i z e d i n that for external packet data network access, the access means (4;41) is connected to a router (5A,5B;51), for Internet access, e.g. an ISP (Internet Service Provider)(5A).

9. An arrangement at least according to claim 8, c h a r a c t e r i z e d i n that the filtering functionality of the filter is provided in the access means (4;41).

10. An arrangement according to any one of the preceding claims, c h a r a c t e r i z e d i n that the filter is defined by the end user (1;11) and in that a number of filtering function attributes are used to define the filter.

11. An arrangement according to claim 10,

c h a r a c t e r i z e d i n
that for setting up a filter, a message signal is provided from the end user station (1;11) to the access means (4;41).

12. An arrangement according to claim 11,
c h a r a c t e r i z e d i n
that a specific message signal is created for end user controlled filter setup.

13. An arrangement according to claim 11,
c h a r a c t e r i z e d i n
that an existing message signal is used for end user controlled filter setup.

14. An arrangement at least according to claim 10,
c h a r a c t e r i z e d i n
that the filtering functionality is positive or negative, i.e. defining either wanted or unwanted information.

15. An arrangement according to claim 10 or 14,
c h a r a c t e r i z e d i n
that the filtering function attributes relate to one or more of source IP address, IP subnet, source port in IP header, source type of protocol in IP header, originating router, e.g. ISP, FTP files etc.

16. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the filter functionality setup presupposes successful connection/attachment of the end user station (1;11) to the backbone network (3;31).

17. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the backbone network comprises a GPRS (UMTS/GPRS) system.

18. An arrangement according to claim 17,
c h a r a c t e r i z e d i n
that the access means is a GGSN (Gateway GPRS Support Node) (41).

19. An arrangement according to claim 18,
c h a r a c t e r i z e d i n
that the existing messaging relating to activation and set up of a secondary PDP context request/response are used to set up a filter in GGSN (41).

20. An arrangement according to claim 19,
c h a r a c t e r i z e d i n
that the message contains information relating to filter attributes, a service class with a context of discarding unwanted data packets (not) meeting requirements given by filter attributes.

21. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the filter is applied on all data packets received in the access means (4;41) and with a destination address corresponding to the end user address.

22. An arrangement according to claim 1,
c h a r a c t e r i z e d i n

that the access means (4;41) comprises/are associated with a firewall, and in that the filter is set up in the firewall.

23. A method of controlling the communication of data between a number of external packet data networks and an end user station in a communication system comprising a backbone network and supporting communication of packet data,
c h a r a c t e r i z e d i n
that it comprises the steps of:
- providing information from the end user station to an external packet data network access node containing requirements relating to wanted/unwanted data information;
- defining and activating information control means comprising a filter in the access node such that only wanted data information is forwarded to the end user, such information control means being remotely controlled by the end user.

24. A method according to claim 23,
c h a r a c t e r i z e d i n
that it comprises the step of:
- creating a new message for providing the information for defining/activating the information control means from the end user station to the access node.

25. A method according to claim 23,
c h a r a c t e r i z e d i n
that it comprises the step of:
- using already existing signalling/messages for providing the information for defining/activating the information control means, between the end user station and the access node.

26. A method according to claim 25,

characterized in
that the backbone network is (UMTS) GPRS and in that it comprises the step of:

- using the messaging relating to requesting and activating a Secondary PDP Context to setup information control means comprising a customized filter in an access node comprising an GGSN.

27. A method at least according to claim 23,
characterized in
that it comprises the step of:

- applying the filter on all data packets received in the access node having the address of the end user having setup the filter as destination address;
- discarding unwanted data packets in the access node.

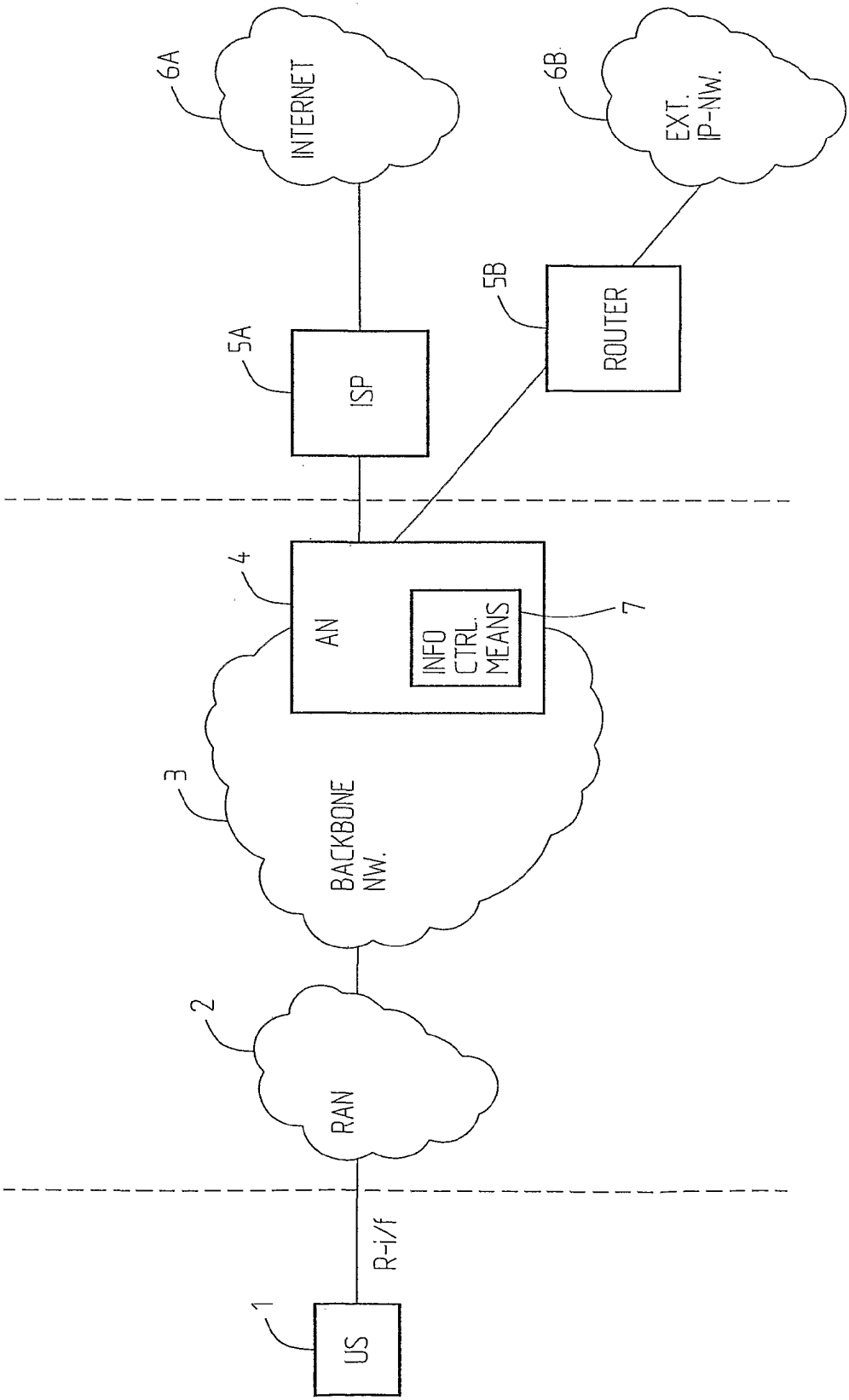

6A
INTERNET
6B
EXT.
IP-NW.
5B
ROUTER
5A
ISP
4
AN
INFO
CTRL.
MEANS
7
3
BACKBONE
NW.
2
RAN
R-i/f
1
US

Fig. 1

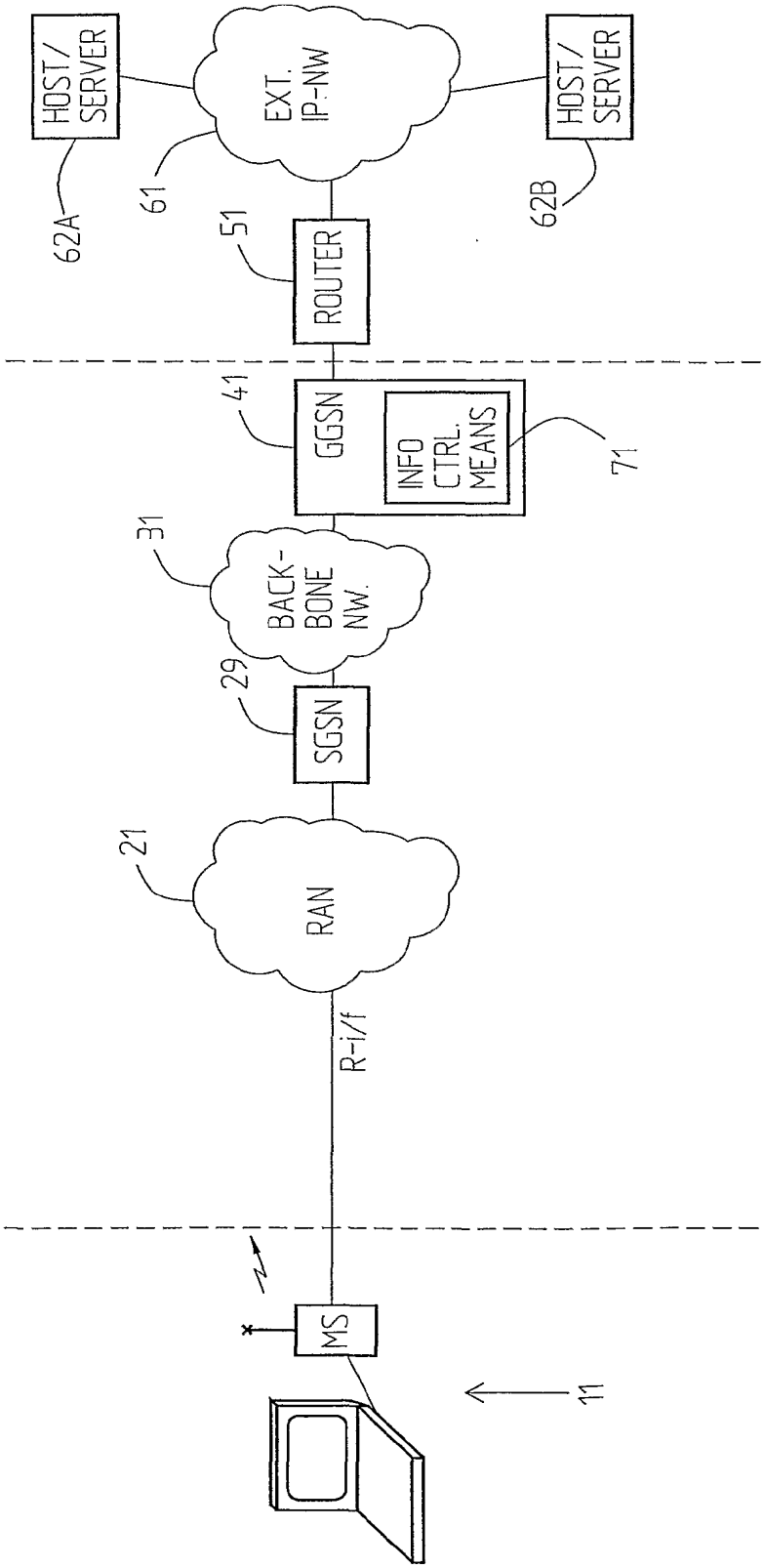

HOST/ SERVER
EXT. IP-NW
HOST/ SERVER
62A
61
62B
51
ROUTER
41
GGSN
INFO CTRL. MEANS
71
31
BACK-BONE NW.
29
SGSN
21
RAN
R-i/f
MS
11

Fig.2

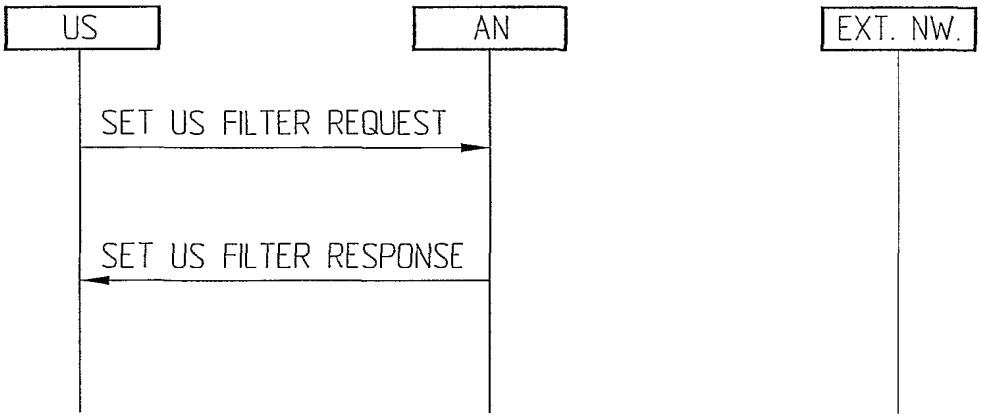


Fig. 3

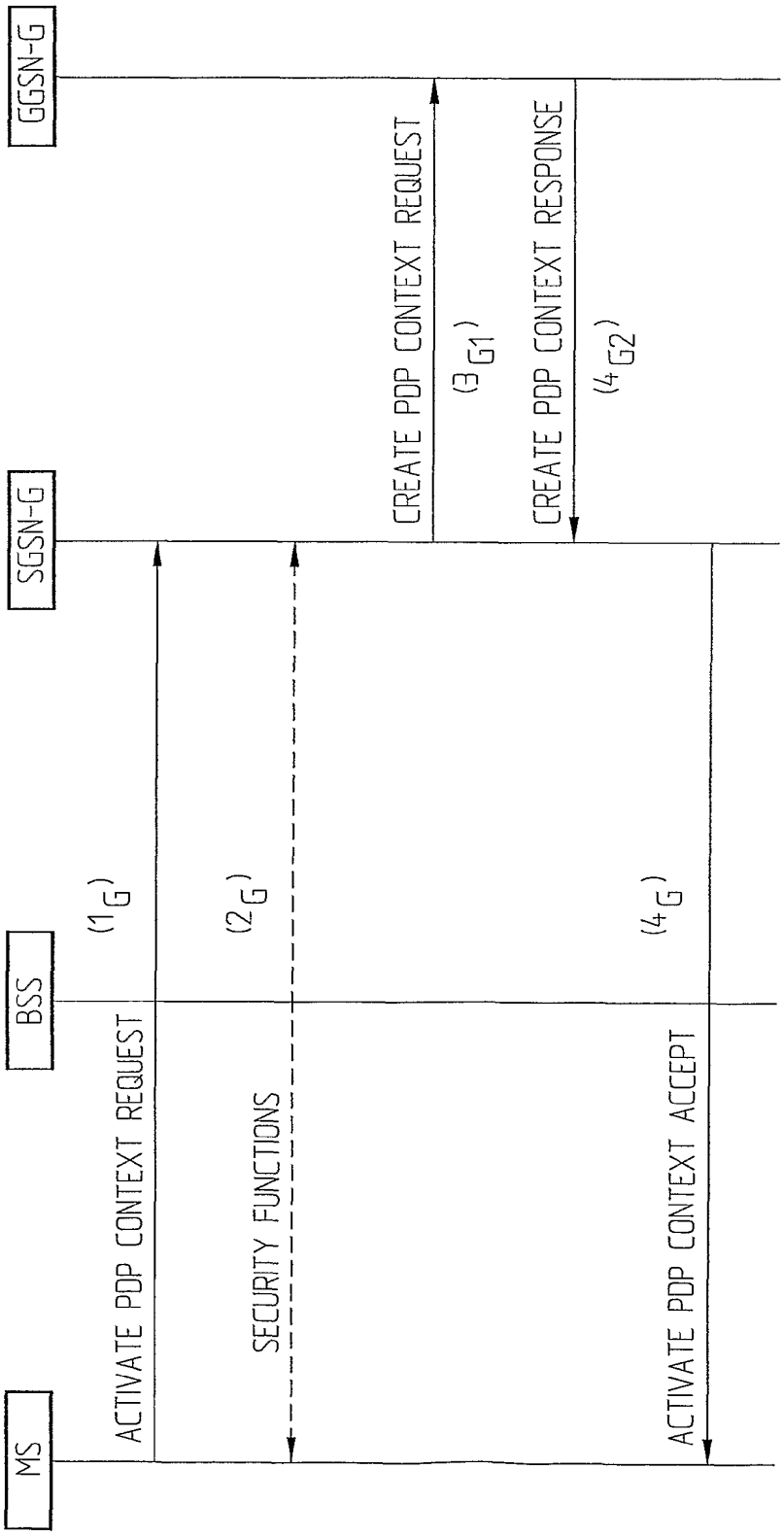

MS
BSS
SGSN-G
GGSN-G
ACTIVATE PDP CONTEXT REQUEST
(1G')
SECURITY FUNCTIONS
(2G')
CREATE PDP CONTEXT REQUEST
(3G1')
CREATE PDP CONTEXT RESPONSE
(4G2')
ACTIVATE PDP CONTEXT ACCEPT
(4G')

Fig. 4

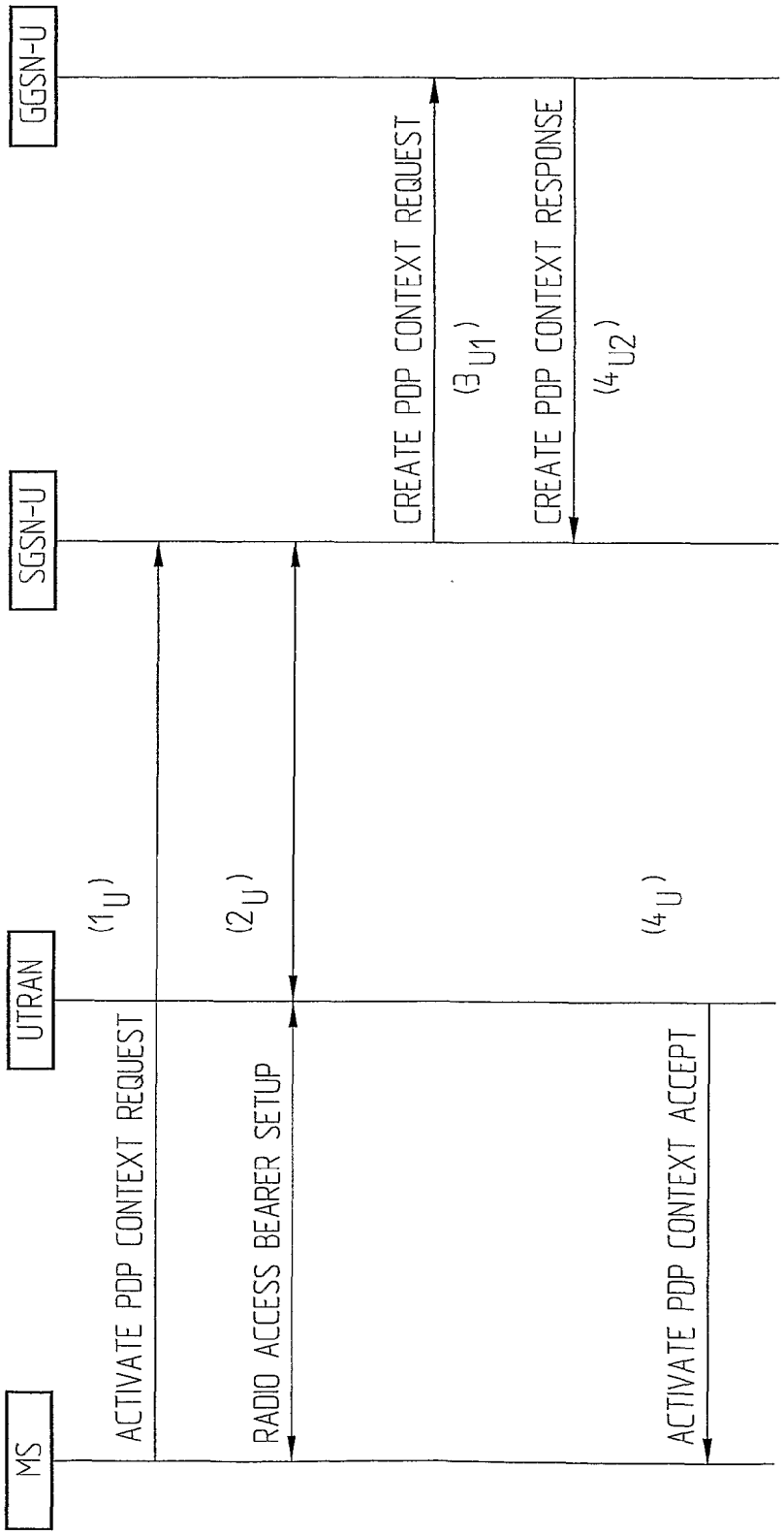

GGSN-U
SGSN-U
UTRAN
MS
CREATE PDP CONTEXT REQUEST
CREATE PDP CONTEXT RESPONSE
(3U1)
(4U2)
(1U)
(2U)
(4U)
ACTIVATE PDP CONTEXT REQUEST
RADIO ACCESS BEARER SETUP
ACTIVATE PDP CONTEXT ACCEPT

Fig. 5

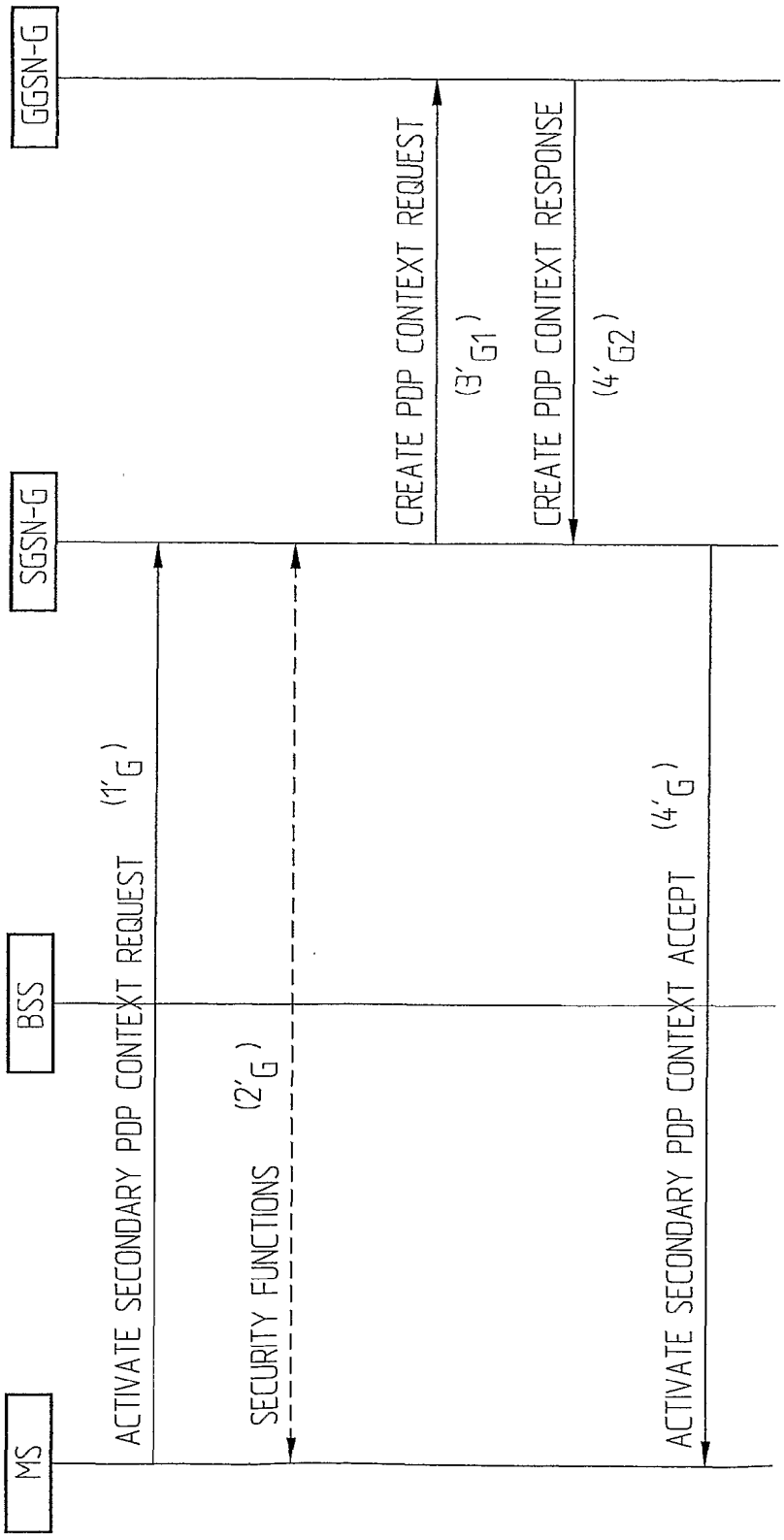

MS
BSS
SGSN-G
GGSN-G
ACTIVATE SECONDARY PDP CONTEXT REQUEST (1'G)
SECURITY FUNCTIONS (2'G)
CREATE PDP CONTEXT REQUEST (3'G1)
CREATE PDP CONTEXT RESPONSE (4'G2)
ACTIVATE SECONDARY PDP CONTEXT ACCEPT (4'G)

Fig. 6

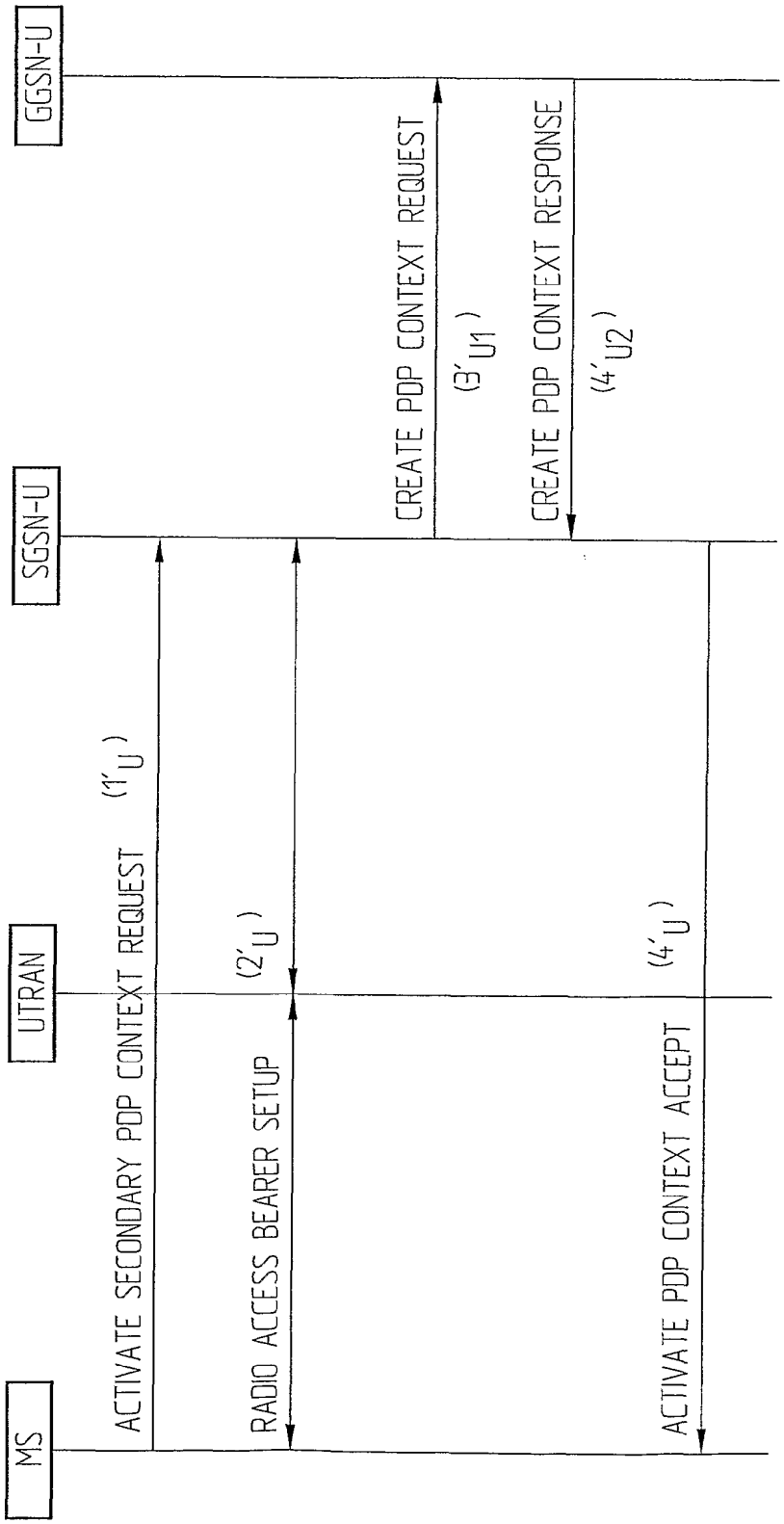

MS
UTRAN
SGSN-U
GGSN-U
ACTIVATE SECONDARY PDP CONTEXT REQUEST (1'U)
RADIO ACCESS BEARER SETUP (2'U)
CREATE PDP CONTEXT REQUEST (3'U1)
CREATE PDP CONTEXT RESPONSE (4'U2)
ACTIVATE PDP CONTEXT ACCEPT (4'U)

Fig. 7

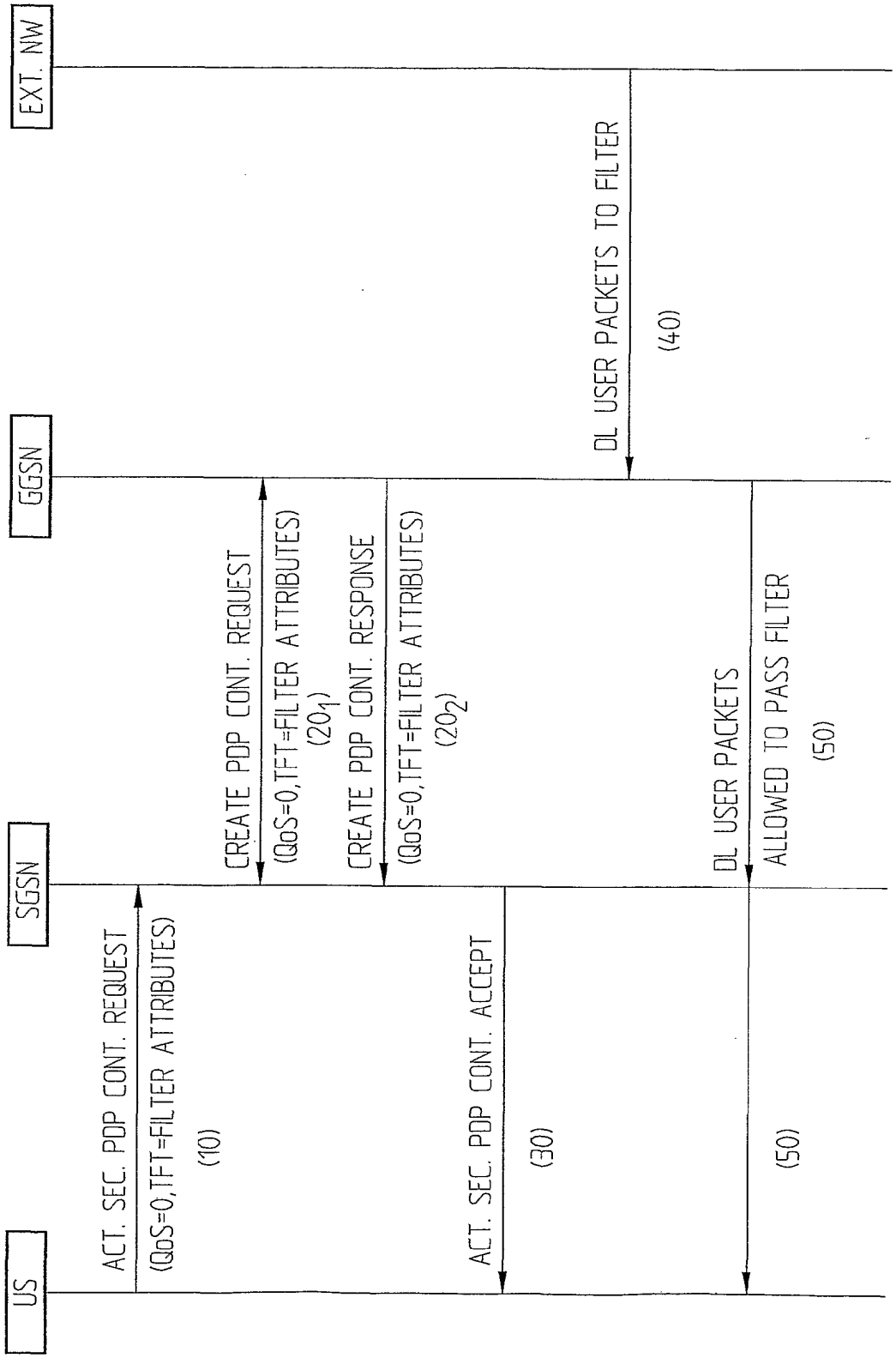

US
SGSN
GGSN
EXT. NW
ACT. SEC. PDP CONT. REQUEST
(QoS=0,TFT=FILTER ATTRIBUTES)
(10)
CREATE PDP CONT. REQUEST
(QoS=0,TFT=FILTER ATTRIBUTES)
(20$_1$)
CREATE PDP CONT. RESPONSE
(QoS=0,TFT=FILTER ATTRIBUTES)
(20$_2$)
DL USER PACKETS TO FILTER
(40)
ACT. SEC. PDP CONT. ACCEPT
(30)
DL USER PACKETS
ALLOWED TO PASS FILTER
(50)
(50)

Fig.8

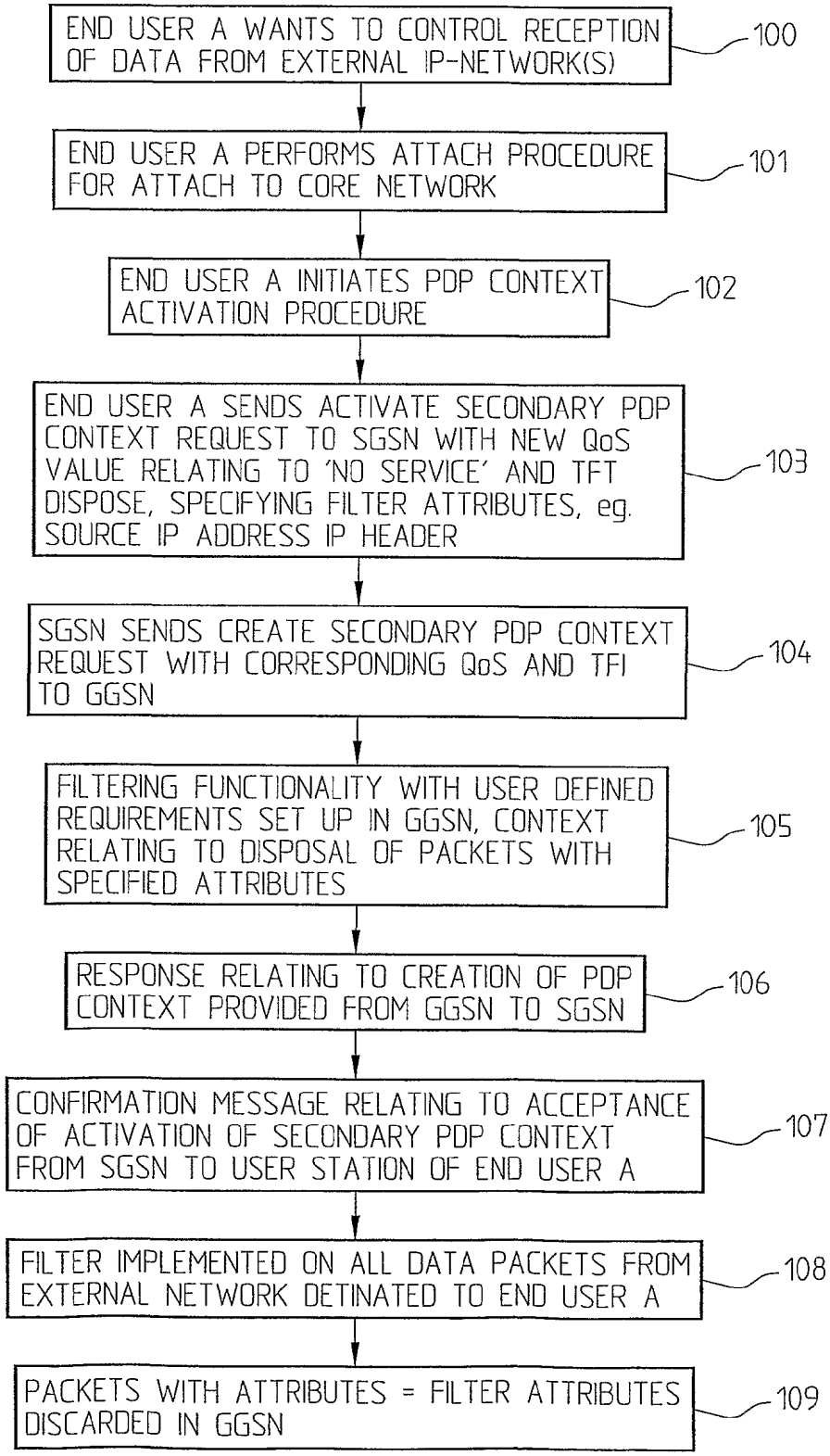

END USER A WANTS TO CONTROL RECEPTION OF DATA FROM EXTERNAL IP-NETWORK(S)
100
END USER A PERFORMS ATTACH PROCEDURE FOR ATTACH TO CORE NETWORK
101
END USER A INITIATES PDP CONTEXT ACTIVATION PROCEDURE
102
END USER A SENDS ACTIVATE SECONDARY PDP CONTEXT REQUEST TO SGSN WITH NEW QoS VALUE RELATING TO 'NO SERVICE' AND TFT DISPOSE, SPECIFYING FILTER ATTRIBUTES, eg. SOURCE IP ADDRESS IP HEADER
103
SGSN SENDS CREATE SECONDARY PDP CONTEXT REQUEST WITH CORRESPONDING QoS AND TFI TO GGSN
104
FILTERING FUNCTIONALITY WITH USER DEFINED REQUIREMENTS SET UP IN GGSN, CONTEXT RELATING TO DISPOSAL OF PACKETS WITH SPECIFIED ATTRIBUTES
105
RESPONSE RELATING TO CREATION OF PDP CONTEXT PROVIDED FROM GGSN TO SGSN
106
CONFIRMATION MESSAGE RELATING TO ACCEPTANCE OF ACTIVATION OF SECONDARY PDP CONTEXT FROM SGSN TO USER STATION OF END USER A
107
FILTER IMPLEMENTED ON ALL DATA PACKETS FROM EXTERNAL NETWORK DETINATED TO END USER A
108
PACKETS WITH ATTRIBUTES = FILTER ATTRIBUTES DISCARDED IN GGSN
109

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01924

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/56, H04L 12/14, H04Q 7/22, G06F 17/60
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04Q, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI DATA, EPO-INTERNAL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9916268 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 1 April 1999 (01.04.99), page 4, line 6 - line 12; page 4, line 20 - line 26; page 5, line 8 - line 15, figure 4 --	1-27
X	DE 19629233 A1 (DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH), 29 January 1998 (29.01.98), abstract, claims --	1-27
X	WO 9933291 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 1 July 1999 (01.07.99), page 5, line 1 - line 9, figure 3 --	1-27

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 December 2001	12 -12- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Kristoffer Ogebjer/LR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01924

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5721827 A (LOGAN, JAMES ET AL.), 24 February 1998 (24.02.98), column 9, line 50 - column 10, line 5	1-16,21-25, 27
A	WO 9923580 A1 (ERICSSON, INC), 14 May 1999 (14.05.99), page 5, line 11 - line 16; page 6, line 1 - line 6; page 7, line 25 - page 8, line 3	1-27
A	WO 9935778 A2 (MICROSOFT CORPORATION), 15 July 1999 (15.07.99), claims	1-27
P,X	WO 0077979 A2 (GEOWORKS CORPORATION), 21 December 2000 (21.12.00), claims, figures	1-27
P,X	WO 0133889 A1 (AMITAI-ORENY, DGANIT), 10 May 2001 (10.05.01), page 5, line 1 - line 2, claims 20,23	1-27
P,X	WO 0101317 A1 (IPOOL CORPORATION), 4 January 2001 (04.01.01), page 36, line 1 - line 6; page 37, line 7 - line 25	1-16,21-25, 27

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SE 01/01924

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9916268 A1	01/04/99	AU 9290098 A	12/04/99
		BR 9812826 A	08/08/00
		CN 1271497 T	25/10/00
		EP 1018276 A	12/07/00
		TW 417406 B	00/00/00
		US 6047194 A	04/04/00
DE 19629233 A1	29/01/98	AT 205322 T	15/09/01
		AU 3846197 A	10/02/98
		DE 59704555 D	00/00/00
		EP 0939945 A,B	08/09/99
		WO 9803951 A	29/01/98
WO 9933291 A1	01/07/99	AU 1989699 A	12/07/99
		GB 0016212 D	00/00/00
		GB 2349779 A	08/11/00
		US 6226523 B	01/05/01
US 5721827 A	24/02/98	NONE	
WO 9923580 A1	14/05/99	AU 9684098 A	24/05/99
		BR 9814112 A	03/10/00
		CN 1301366 T	27/06/01
		EP 1027668 A	16/08/00
WO 9935778 A2	15/07/99	EP 1051681 A	15/11/00
		EP 1051823 A	15/11/00
		EP 1051824 A	15/11/00
		EP 1053525 A	22/11/00
		EP 1058874 A	13/12/00
		EP 1060597 A	20/12/00
		US 6118391 A	12/09/00
		US 6282294 B	28/08/01
		US 6289464 B	11/09/01
		WO 9935557 A	15/07/99
		WO 9935591 A	15/07/99
		WO 9935593 A	15/07/99
		WO 9935801 A	15/07/99
		WO 9935802 A	15/07/99
		EP 0913942 A	06/05/99
		JP 11234115 A	27/08/99
		SG 68690 A	16/11/99
		US 6114895 A	05/09/00
		US 6285236 B	04/09/01
		AU 3789000 A	29/05/00
		WO 0027533 A	18/05/00
WO 0077979 A2	21/12/00	AU 5740500 A	02/01/01
WO 0133889 A1	10/05/01	AU 1046201 A	14/05/01
WO 0101317 A1	04/01/01	AU 5782000 A	31/01/01